PD6 Exh 21

OCEG®

DRIVING PRINCIPLED PERFORMANCE®

2015 GRC MATURITY SURVEY

HOW THE APPROACH TO GRC STRATEGY & INTEGRATION AFFECTS CONFIDENCE

About OCEG . . .

OCEG is a non-profit think tank that helps organizations achieve Principled Performance. We provide standards, resources and a hub around which many professionals collaborate including: board members, business executives and operators, risk executives, audit executives, compliance executives, financial executives, IT executives, and HR executives.

Our mission is to help organizations reliably achieve objectives while addressing uncertainty and acting with integrity – this is Principled Performance. We assist organizations in developing and implementing GRC capabilities that enable Principled Performance by providing authoritative resources for integrating the governance, assurance and management of performance, risk and compliance. OCEG's global community exceeds 40,000 members and through collaborative effort we continue to advance methods and measurements of success on the path to Principled Performance.

For more information:

www.OCEG.org

info@OCEG.org

OCEG®

DRIVING PRINCIPLED PERFORMANCE®

Survey Analysis by . . .

GRC 20/20 Research, LLC provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective research and benchmarking. We provide independent and objective insight into leading GRC practices and processes, including market dynamics and intelligence; risk, regulatory and technology trends; competitive landscapes; market sizing; expenditure priorities; and RFP development and support.

For more information:

www.GRC2020.com

info@GRC2020.com

grc2020

PREFACE

If you are taking the time to read this survey, it is likely you have a certain level of interest in governance, risk management, and compliance (GRC). There's no shortage of information on the subject. An Internet search will throw up all sorts of tips, views and best practices designed to help organizations and the many roles responsible for aspects of GRC.

OCEG is the framework body for GRC. We advocate Principled Performance and the role of GRC to enable organizations to reliably achieve objectives while addressing uncertainty and acting with integrity. Our mission is to help organizations achieve Principled Performance by providing a community and authoritative resources for integrating governance, assurance and management of performance, risk, compliance and ethics.

OCEG is the only organization that focuses on Principled Performance and integrating the governance, assurance and management of performance, risk, compliance and ethics (GRC). By integrating these areas, organizations simultaneously increase performance, address risk and reduced costs. As a non-profit that does not represent a specific profession, we are uniquely positioned to serve as a hub around which many professions can collaborate on solutions.

This OCEG 2015 GRC Maturity Survey report takes a look at how organizations are taking varying approaches to GRC from the siloed to the fully integrated and measures the satisfaction and confidence organizations have as a result.

We hope this survey report provides you with valuable insights to improve GRC strategy, processes, and architecture within your organization.

Survey data can be downloaded at:
http://www.oceg.org/resources/oceg-2015-grc-maturity-survey-data-sets/

Table of Contents

OCEG 2015 GRC Maturity Survey Sponsor

The 2015 OCEG GRC Maturity Survey is made possible through the support of the entire OCEG GRC Solutions Council and particularly the following survey sponsor:

All organizations, big and small, have processes to address their governance, risk management, and compliance (GRC) obligations. Some have highly sophisticated, integrated processes, while others rely on informal, disjointed processes. We refer to these less sophisticated processes as "siloed" because they often behave in inconsistent ways and produce inconsistent results.

Independent research finds that structured and integrated GRC programs are consistently more efficient and effective—achieving objectives, addressing risks, and acting with integrity. However, despite the obvious value that integrated programs bring, GRC processes remained siloed and inefficient in many organizations around the world.

OCEG and its partners set out to understand the progress that companies have made in recent years and the impact of those efforts. The results have been compiled in this insightful 2015 GRC Maturity Survey Report.

As you will see, organizations have made substantial progress in recent years, but problems remain. The solution to these problems is clear: technology and collaboration.

With a greater emphasis on technology and collaboration within GRC processes, organizations can begin to reduce inefficiencies and uncontrolled risk through integration. By doing so, risk management and compliance professionals can better identify and understand the risks present within their organizations—and share with others how to address the risks and achieve performance goals.

Joseph Howell
Co-Founder, Executive Vice President
Workiva

Workiva (NYSE: WK) created Wdesk, a cloud-based platform for enterprises to collect, manage, report, and analyze business data in real time. Wdesk includes a sophisticated productivity suite for business data collaboration and reporting that is used by thousands of corporations, including more than 65 percent of the Fortune 500. See what we can do for you at workiva.com.

INTRODUCTION – Every Organization Does GRC

Greetings,

Every organization does GRC whether they use the acronym or not. All have some approach to governing the organization, managing risk, and addressing compliance. It could be scattered in silos and disconnected, or it could be highly collaborated and integrated. Organizations should not be asking if they should do GRC but are to ask how mature their organization's approach to GRC is and how it can be improved.

The formal definition for GRC found in the OCEG GRC Capability Model is that "GRC is a capability to reliably achieve objectives [governance] while addressing uncertainty [risk management] and acting with integrity [compliance]."

In the ideal world there is a natural flow through to GRC. Governance sets objectives and directs and steers the organization setting the context for risk management. Risk management aims to understand and minimize uncertainty in those objectives and reduce exposure to loss while maximizing performance. Compliance assures that the organization operates with integrity to the boundaries established in organization values, policies, regulatory and legal requirements, as well as boundaries set by risk limits and thresholds.

However, within many organizations there are often many GRC functions operating in isolation producing redundancy and gaps while remaining ignorant of the interrelationship of risk across silos. This has a measurable cost to the organization in inefficiency, ineffectiveness, and lack of agility.

Other organizations have mature and structured processes and reporting on GRC that brings together an integrated and orchestrated view of GRC processes and information.

The goal of this 2015 OCEG GRC Maturity Survey report is to help organizations:

- ***Understand*** the level of integration of GRC within organizations;
- ***Differentiate*** the degree of confidence in performance with the ability to identify and manage risks and requirements;
- ***Examine*** the benefits of an integrated GRC capability and the negative effects of siloed operations.

Michael Rasmussen
OCEG Fellow & Chair of OCEG GRC Solutions Council
The GRC Pundit @ GRC 20/20 Research, LLC
mrasmussen@oceg.org
mkras@grc2020.com

SURVEY DEMOGRAPHICS

Balanced Responses From Industries and Roles

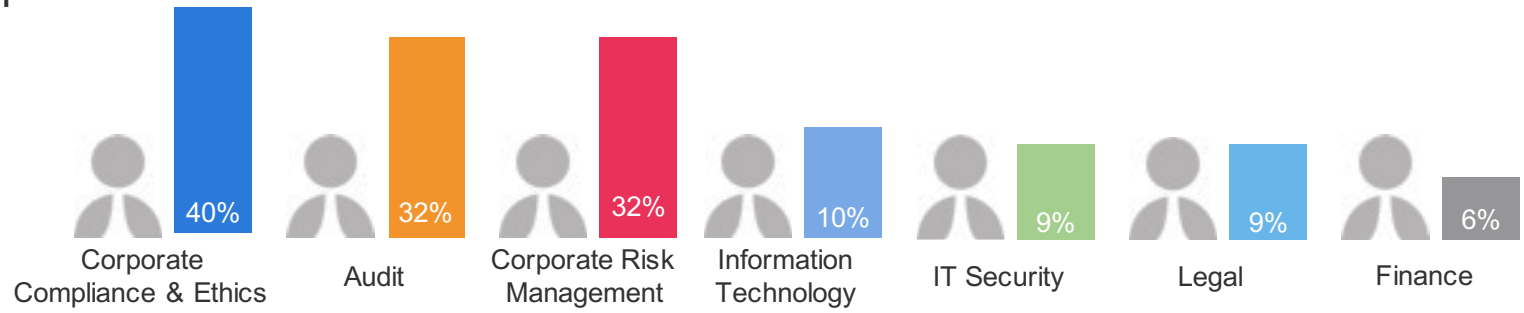
Respondents Have A Broad Range of Responsibilities

There are 370 fully completed responses to the 2015 OCEG GRC Maturity Survey. The majority of these, and the focus of this report, are from the 296 respondents that were from organizations that represented internal roles of GRC. [1] There are an additional 226 partial responses for a survey total of 596 partial to fully completed responses.

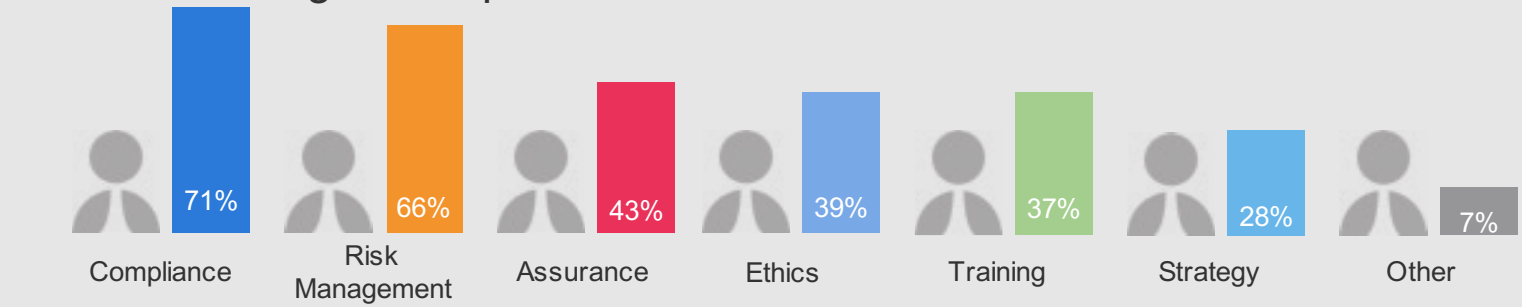
The 296 responses evaluated in this report are from a range of roles/departments in organizations. The three primary areas of responsibility are corporate compliance & ethics (40%), audit (32%), and risk management (32%). Within the roles responding we find that they actually have a diverse set of responsibilities.

1 Responses from GRC solution providers and professional service firms are not included in this report but are available from OCEG.

Respondents are from these business functions . . .



But also have a range of responsibilities . . .



Respondents by Geography

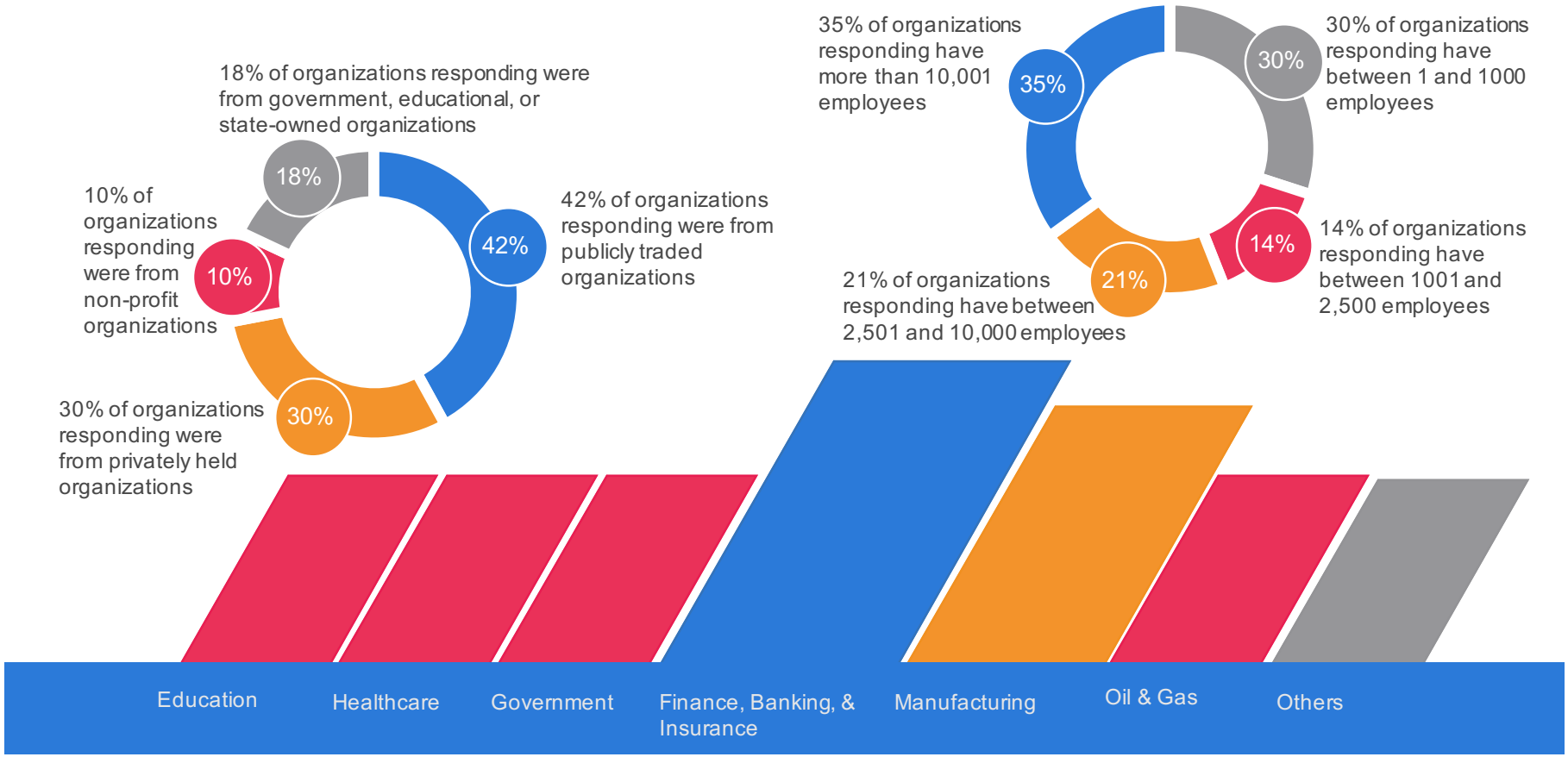
The 296 survey responses represent a diverse geographic distribution with the majority coming from United States & Canada (58%) followed by Europe (18%). The remaining respondents are distributed across other regions of the world.

Respondents by Entity Type, Size & Industry

Organizations responding represent a distributed balance of size and structure, with publicly traded organizations having the largest representation (42%) followed by privately-held organizations (30%).

The survey benefits from a strong response of organizations of varying size. Organizations with over 10,000 employees represent the largest segment of response (35%) followed by small organizations with under 1,000 employees (30%).

A variety of industries are present in the responses with financial services having the strongest representation.



MEASURING GRC MATURITY

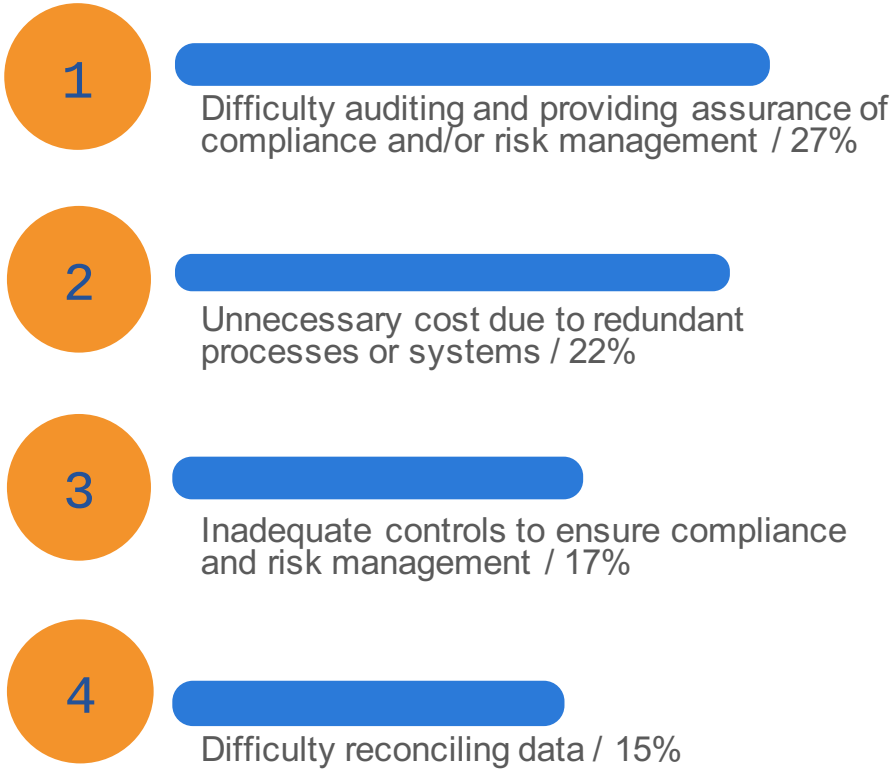
From Silos to Integrated GRC

Impact of Silos and Segregation

The greatest challenge in organization is inconsistent processes, and in that context information, scattered across the organization. Respondents indicated that these redundant and inconsistent processes lead to difficulty in auditing and providing assurance in the context of compliance and risk management (27%) and eventually cause inefficiency in human and financial capital resources due to redundant systems and processes (22%).

Others indicate inadequate controls to ensure compliance and risk management (17%) as well as difficulty reconciling data (15%).

In what ways is your organization adversely impacted by redundant or inconsistent processes for governance, assurance and/or management of performance, risk and compliance?



DATA: all 296 respondents, another 10% stated they were not adversely impacted, and 9% were unsure.

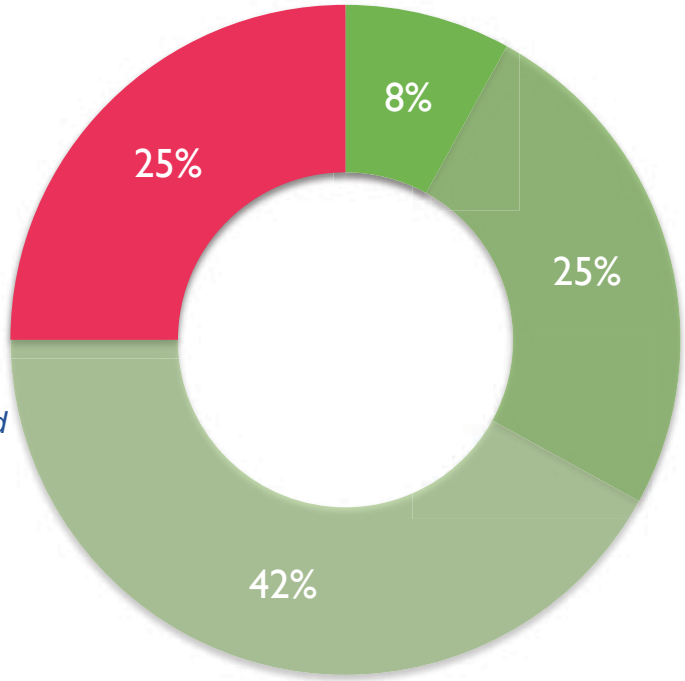
GRC Approach – From Silos to Integrated

The critical pivot of the survey results stems from the question on GRC integration. Twenty-five percent of organizations responding state that their GRC processes largely remain in silos of processes and technologies. On the flip-side of this, seventy-five percent of organizations indicate some level of GRC integration. This includes eight percent that report the majority of their processes and technology are integrated, with twenty-five percent reporting significant progress in GRC integration, and forty-two percent stating they have standardized in some areas of GRC but not all of them.

This question is critical to the results of the rest of the survey as we pivot the siloed responses (25%) and contrast them to the varied stages of integration responses (75%) to measure the impact of GRC integration.

Pick the statement that best describes your organization's state of integration of GRC capabilities.

NOTE: The more integrated you are, the more you share information and use standardized approaches to how you manage and provide assurance about performance, risk and compliance.



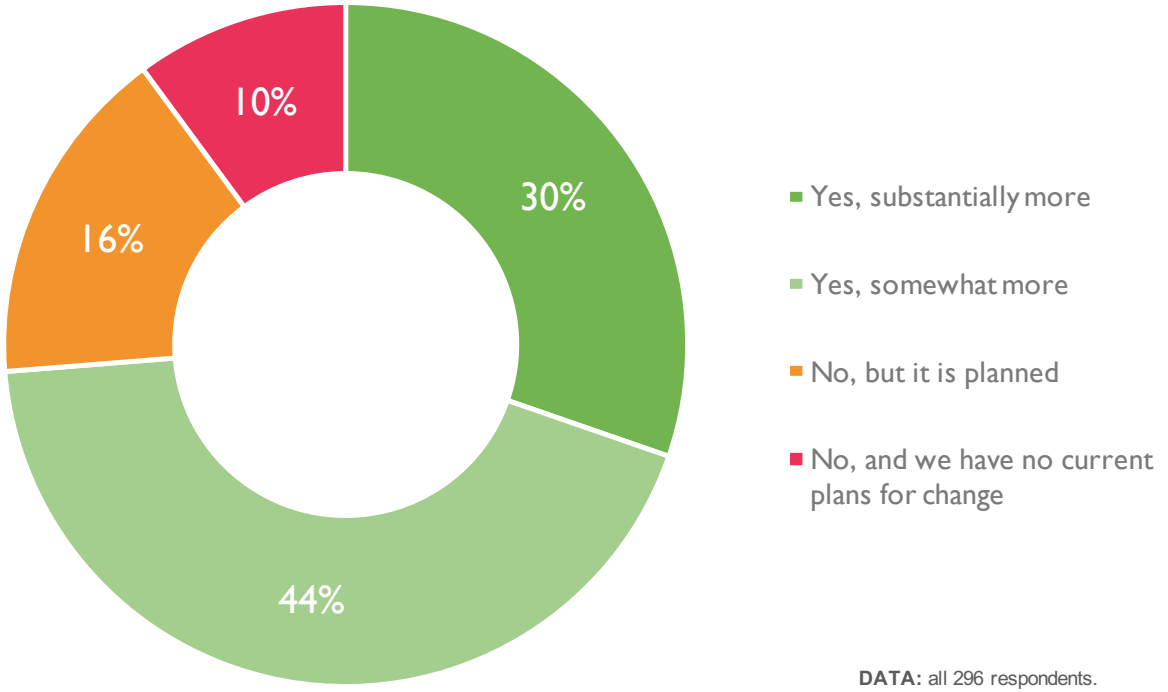
DATA: all 296 respondents.

GRC Integration: Now Compared to Three Years Back

When asked about the current state of GRC integration now compared to three years back the survey reveals that seventy-four percent of respondents indicate they are more integrated (30% substantially more, and 44% somewhat more). Only ten percent indicate they have no change in level of GRC integration over past three years and have no plans to change, while another 16% who have not yet changed have plans to do so.

Interestingly, organizations reporting they are predominantly siloed still indicate (34%) that they have more GRC integration than they did three years ago. This is an indicator on increased awareness and collaboration on GRC even when GRC responsibilities still remain siloed and uncoordinated.

Is there greater GRC integration in your organization today than there was three years ago?



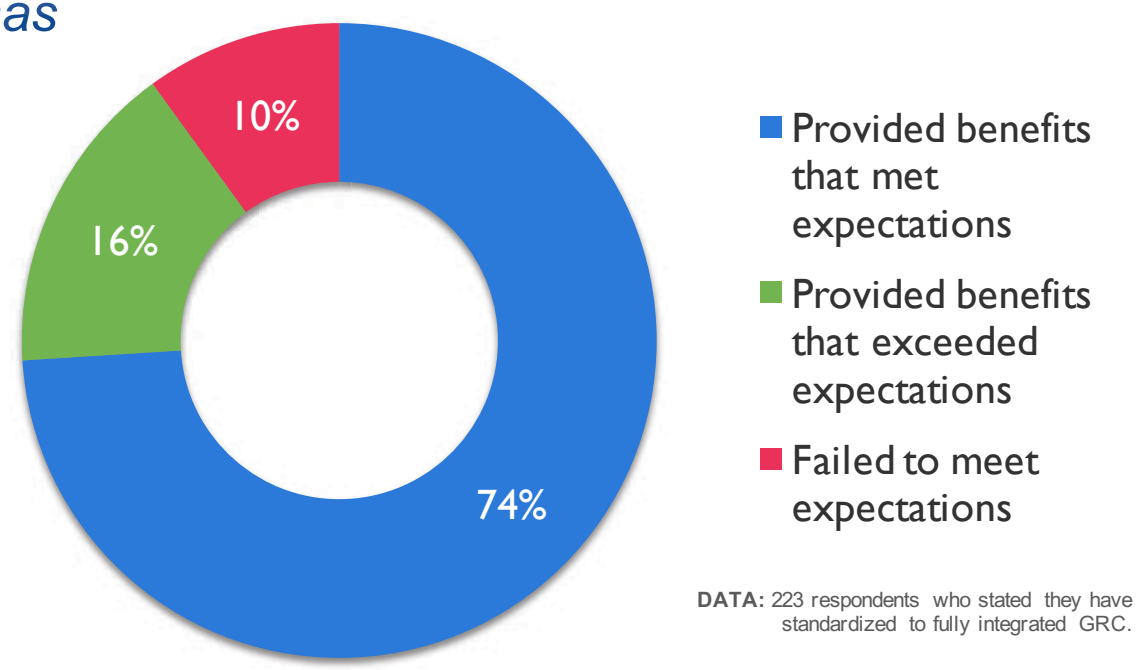
DATA: all 296 respondents.

Benefits & Value Achieved Through GRC Integration

Of the 296 total respondents, 223 (75%) indicate they have some level of GRC standardization and integration across their organization.

Of these 223 respondents with integrated GRC strategies, seventy-four percent state that integration provided benefits that met expectations, while sixteen percent indicate integration exceeded expectations, and only ten percent say that they failed.

Where your organization has integrated processes for governance, assurance and/or management of performance, risk and compliance (GRC), the results have:



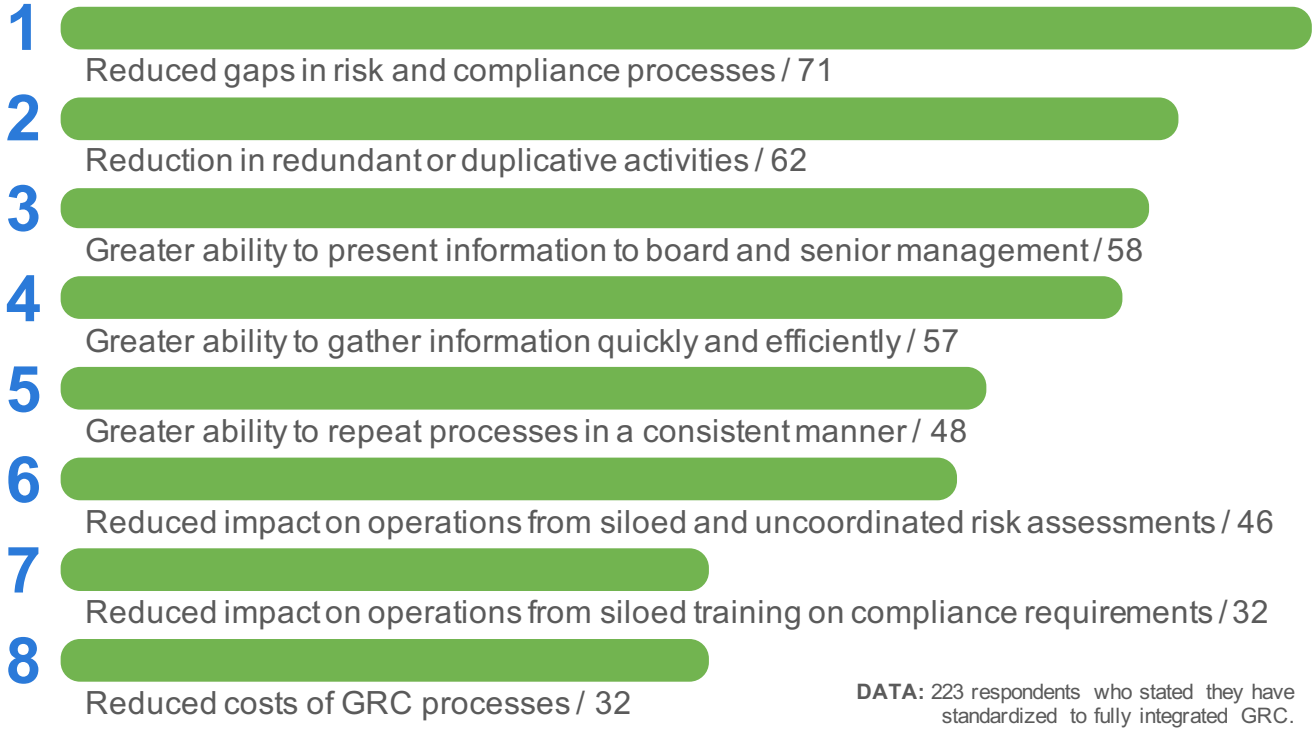
DATA: 223 respondents who stated they have standardized to fully integrated GRC.

Where GRC Value is Achieved Through Integration

Organizations indicating they have standardized to integrated GRC processes report a range of value and specific benefits this has brought to their organization. The most significant benefits are reduced gaps in GRC processes as well as reduction in redundancy of duplicated activities and processes. This indicates increased effectiveness in GRC capabilities in organizations with integrated GRC.

These organizations also report increased ability to gather and report on GRC information, present GRC information to stakeholders, and to repeat processes consistently. This illustrates that integrated GRC brings greater agility to the organization.

Organizations with integrated GRC also report reduced impact on operations and costs of GRC processes which means that integrated GRC brings greater human and financial capital efficiency to the organization.

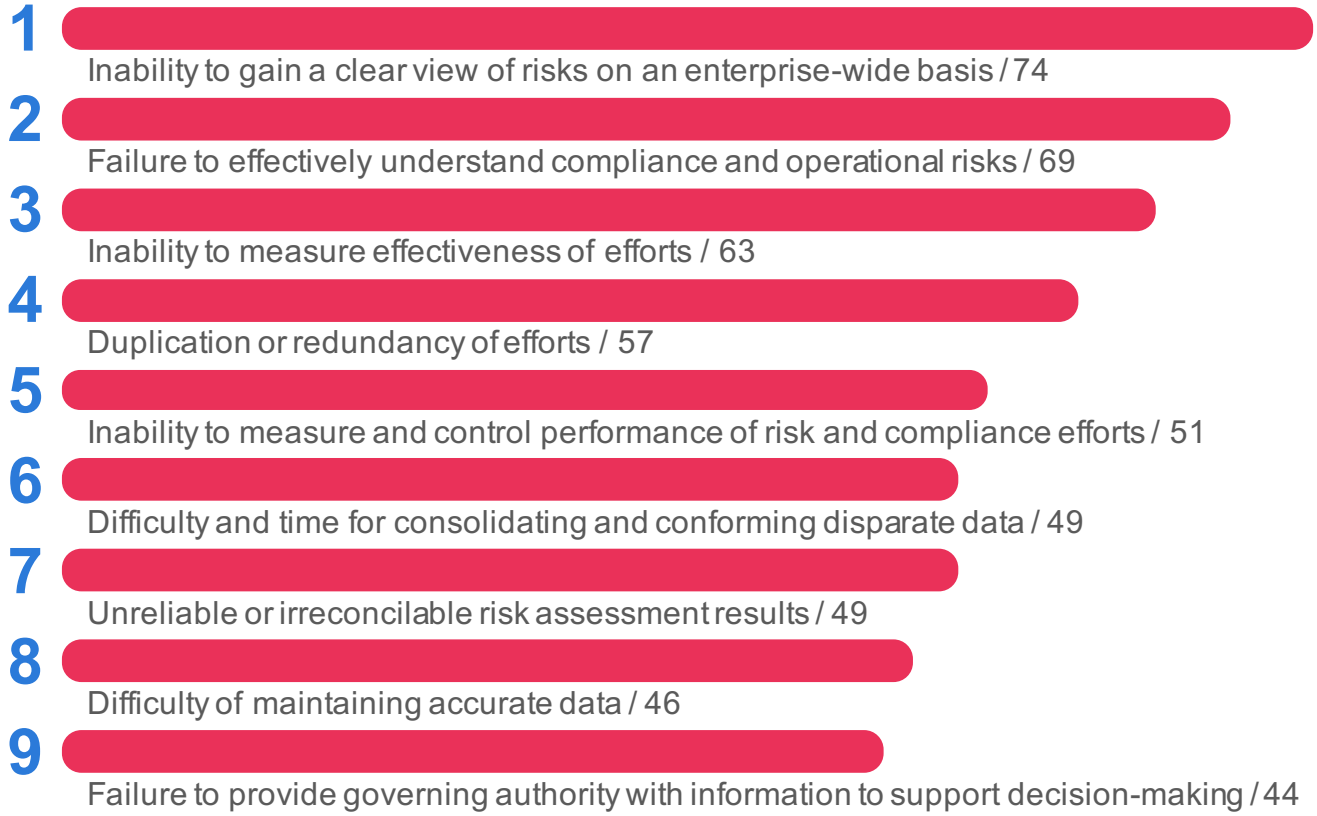


DATA: 223 respondents who stated they have standardized to fully integrated GRC.

The Negative Impact of Silos of GRC

On the flip-side, 25% of organizations responding have predominantly siloed GRC operations scattered across the organization which they state has negatively impacted their organization.

The number one issue is the inability to gain a clear view of risks across the enterprise, and in that context a failure to effectively understand those risks. Several reported a range of challenges including redundancy and difficulty in measuring, gathering data and reporting on GRC information and activities.



DATA: 73 respondents who stated they have siloed GRC processes.

Barriers to GRC Integration

Organizations that lack an integrated GRC strategy clearly indicate that their number one barrier to an integrated GRC strategy is the lack of a champion to advocate collaboration across organizational departments with GRC responsibilities.

The rest of the barriers to GRC integration can all be mapped back to the lack of a champion to facilitate GRC collaboration and integration. These include challenges in getting departments to work together, strategy, and defining a business case for GRC integration.

DATA: 73 respondents who stated they have siloed GRC processes.

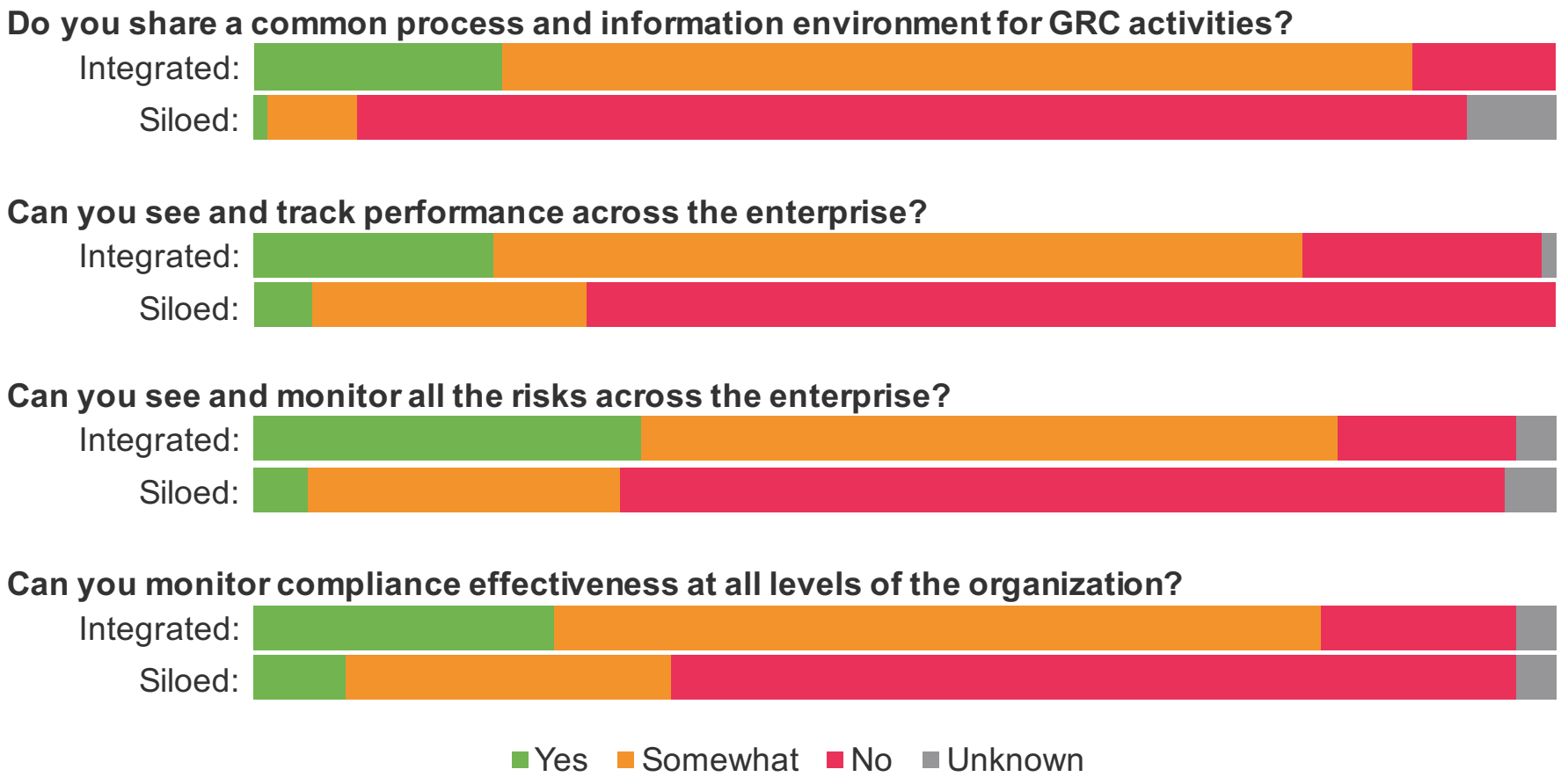
COMPARISON & ANALYSIS

GRC Integration Improves Alignment & Confidence

Integration vs. Silos in GRC Processes & Activities

The positive impact of standardized and integrated GRC is apparent in the consistency in GRC processes and activities when compared to silos.

Not surprisingly, organizations with an integrated GRC strategy report they have common process and information for their GRC environment while silos indicate a lack of common processes and information. This impacts the organization's ability to see and track performance, monitor risks, and monitor compliance across the enterprise with integrated GRC organizations stating they have the capabilities to do so while silos indicate they cannot.

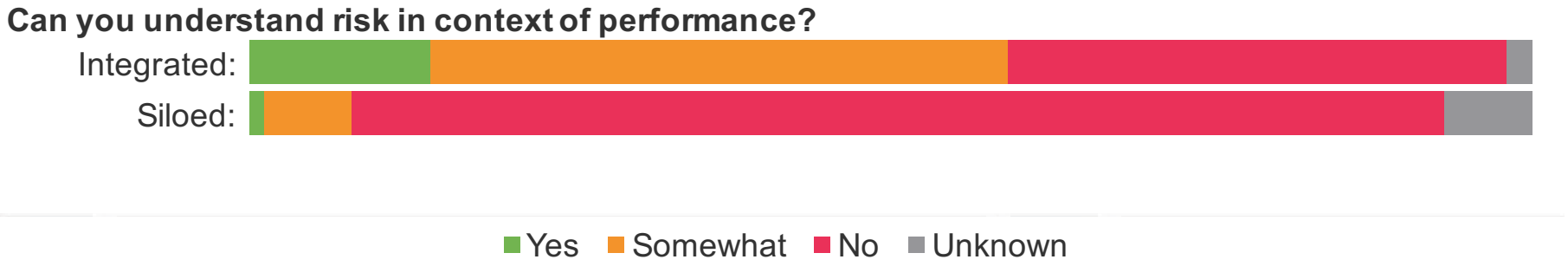


Alignment of Risk to Performance

Building on the same questions on the previous page, is the ability to understand risk in context of performance. The vast majority of organizations with siloed GRC activities indicate they do not have the capabilities to manage and understand risk in context of performance while the majority of organizations with integrated GRC strategies indicate they have capabilities to align risk and performance.

When risk is disconnected from performance and objectives of the organization it operates in a vacuum. The governance function of setting objectives and in that context performance goals and metrics gives context to risk management. Without this context silos of risk management are like a ship adrift at sea with nothing to guide it and give context to the journey.

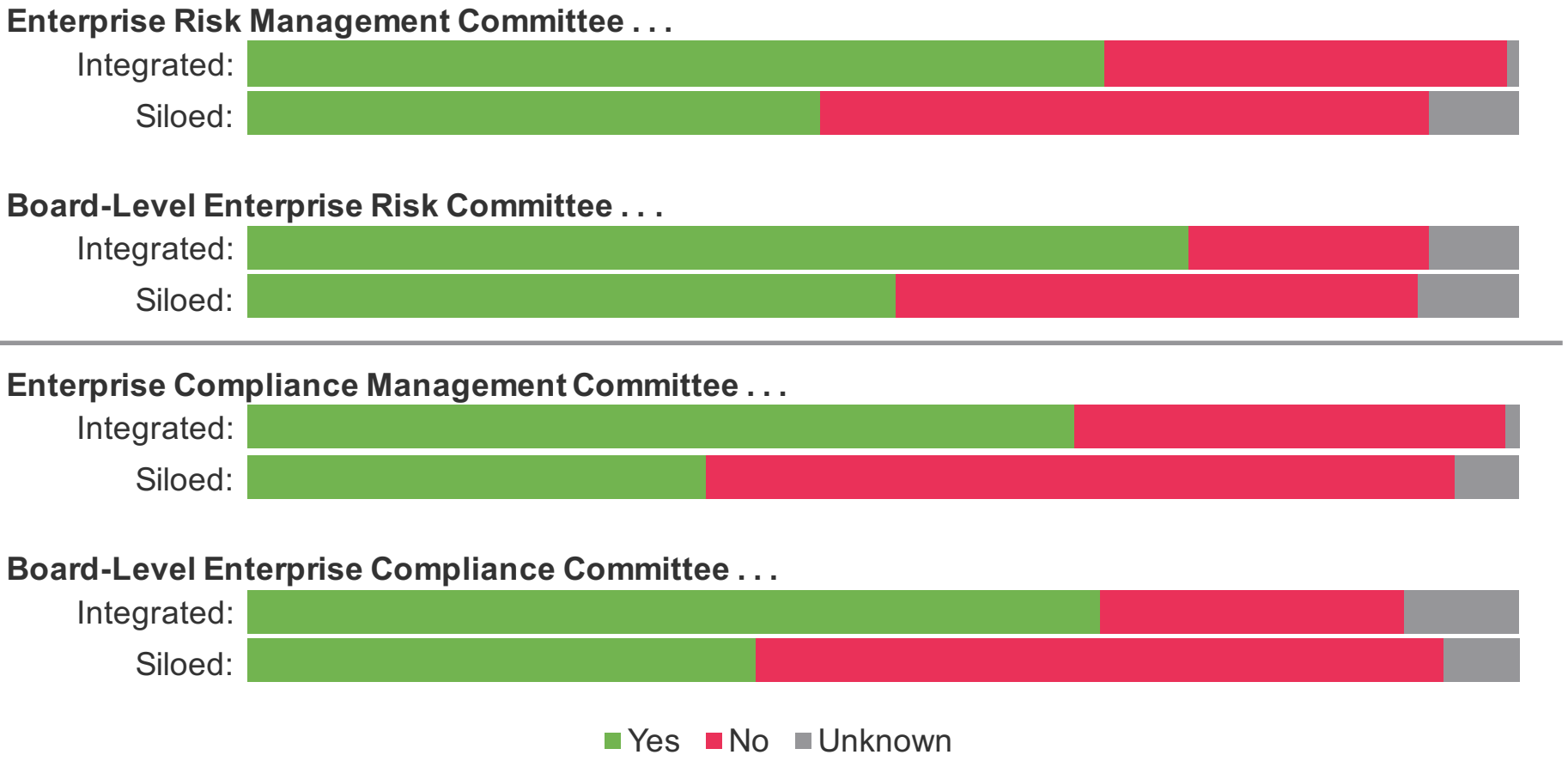
This is one of the most startling and revealing findings of the survey and a significant value statement as to why integrated GRC provides value to the organization.



Presence of GRC Management & Board Committees

Organizations with varying degrees of integrated GRC processes and information show a greater tendency to have enterprise management and board-level committees to govern risk management and compliance.

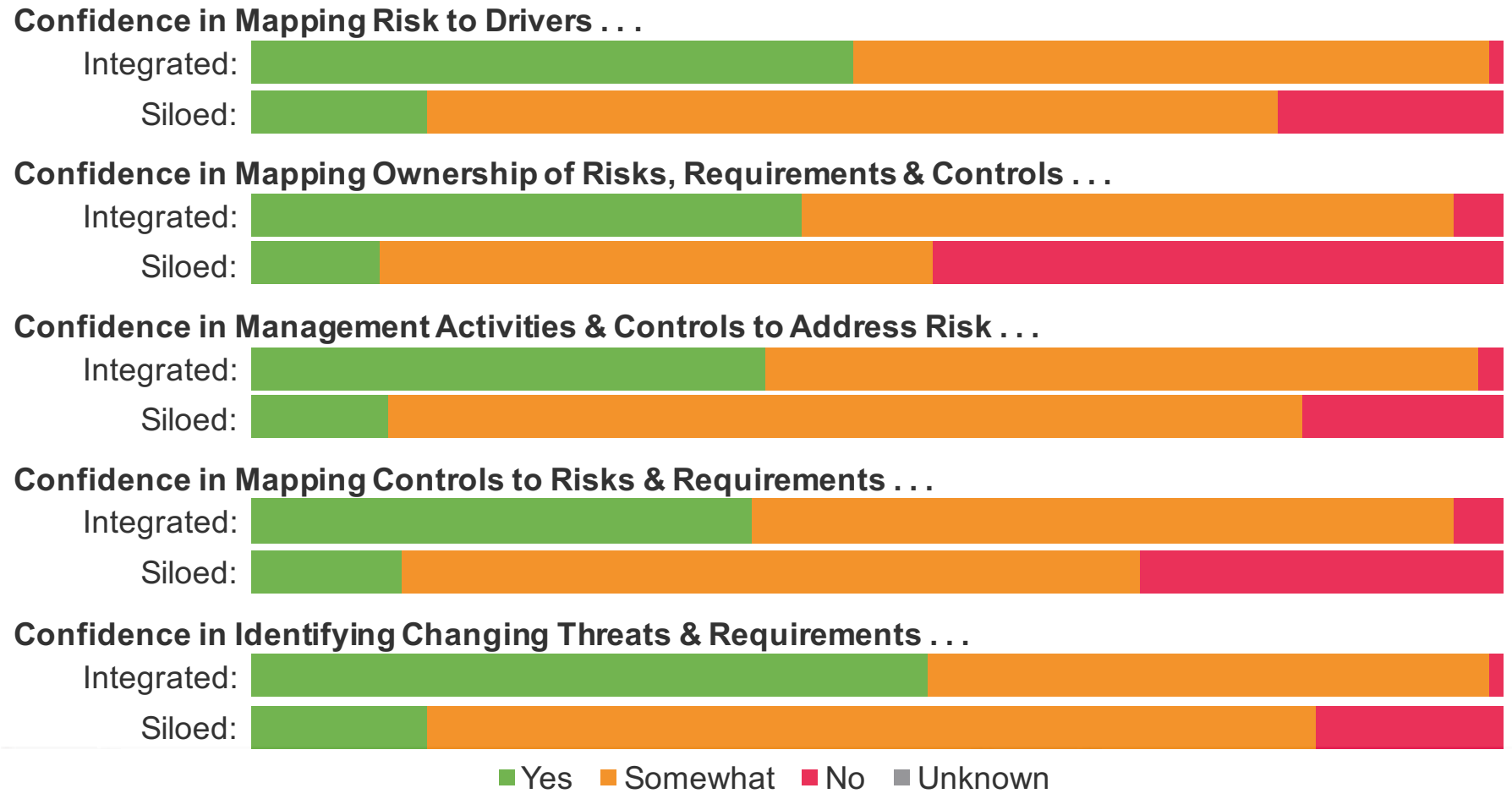
This is a natural outcome of GRC integration as there is greater interest in collaboration and coordination of risk and compliance with prime directive of enterprise and board-level communications and reporting.



GRC Confidence Levels

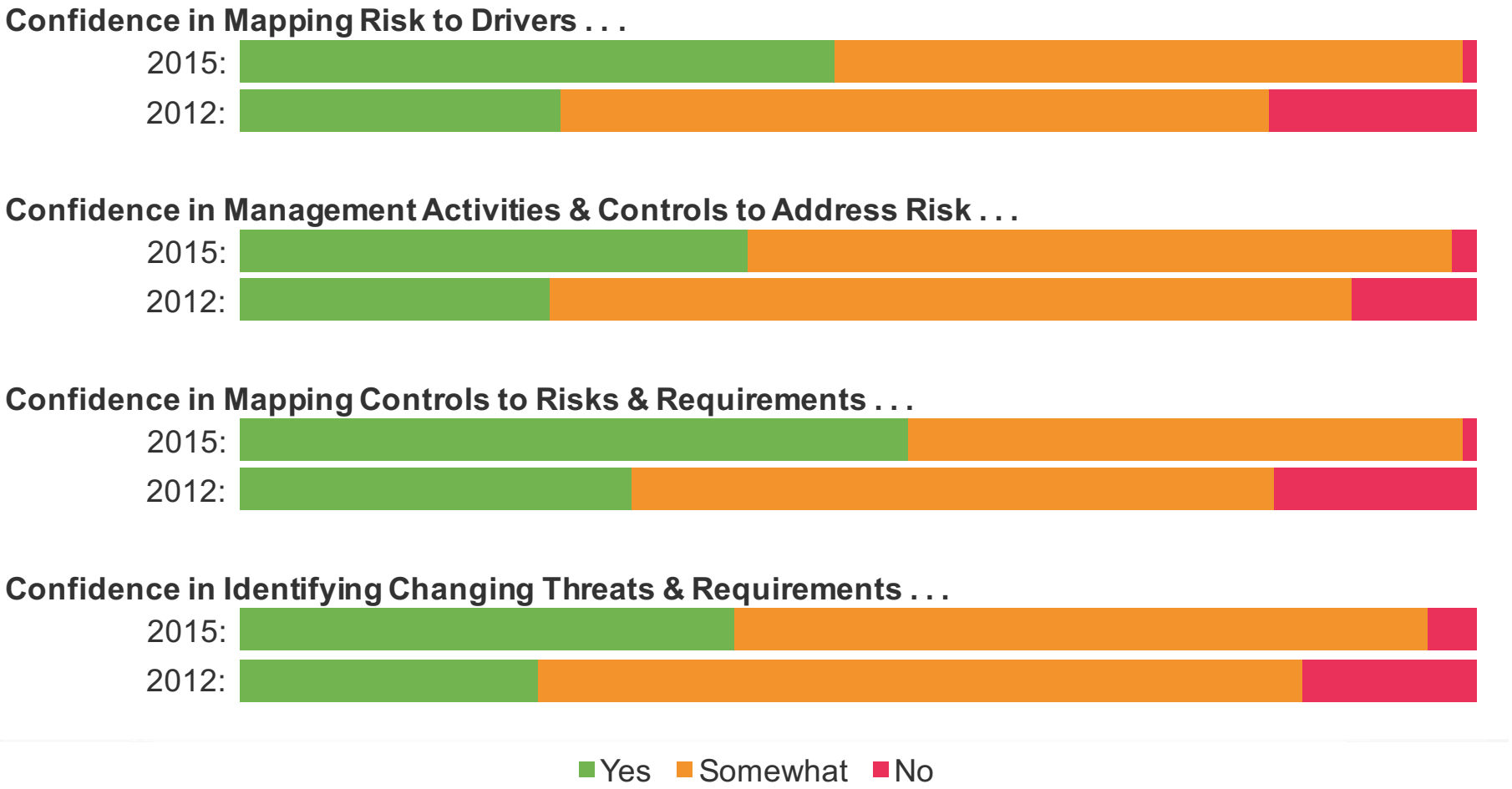
Another revealing finding is the significant disparity between silos and integrated GRC strategies in the context of confidence. Organizations with standardized to integrated GRC show significantly increased confidence in mapping risks and controls, GRC activities, and the ability to identify changing threats and requirements in a dynamic environment.

Organizations with silos of GRC report a general lack of confidence in these respective areas.



Growing Confidence: 2015

Organizations with standardized to integrated GRC processes and activities report greater confidence in GRC capabilities in 2015 than they did in 2012. Over the past three years the degree of confidence in mapping risks and controls, identifying changes, and GRC management activities has become stronger within organizations.



SUMMARY

GRC Integration is the Measurement of GRC Maturity

GRC Integration is the Measurement of GRC Maturity

In the survey results, we find six key take aways that illustrate the value of an integrated approach to GRC and the consistency and confidence senior executives and business management have in the context of GRC.

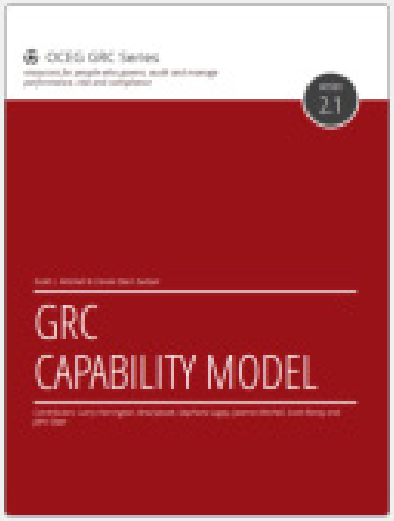
These core points illustrate how GRC integration helps to standardize the measures used across silos, which in turn provides a common framework for comparisons and increased visibility into measures of performance, risk management and compliance across the organization. Further, efficiencies that come from an integrated program (e.g., leveraging a common assessment or analysis instead of doing three separate ones) increases participation and buy-in from the business, which results in higher quality metrics.

1	The more integrated, the greater the ability to manage risk in the context of performance and objectives.
2	The more integrated, the more confident the organization is in GRC processes and capabilities to manage risk and controls, and identify changing threats and requirements.
3	The more integrated, the more collaboration and oversight of risk and compliance at the board level as well as enterprise management committee levels.
4	The more integrated, the more agile the organization is to adapt to changing risk, regulatory, and business environments.
5	The more integrated, the more effective the organization is at managing risk in context of business performance and objectives.
6	The more integrated, the more efficient the organization is in use of human and financial capital to manage GRC activities and processes.

REFERENCES

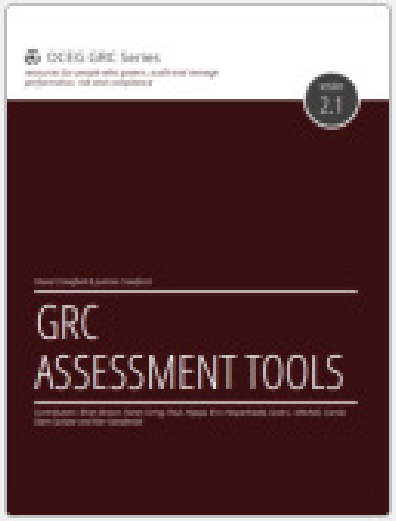
OCEG's GRC Standards Library

OCEG's GRC Standards Library helps to jump-start and improve your approach to achieving Principled Performance.



GRC Capability Model (Red Book)

OCEG worked with a committee of hundreds of esteemed experts, including many in-house GRC professionals, external advisors and auditors, and academics, to develop the OCEG Red Book, which contains the GRC Capability Model™ - the ...

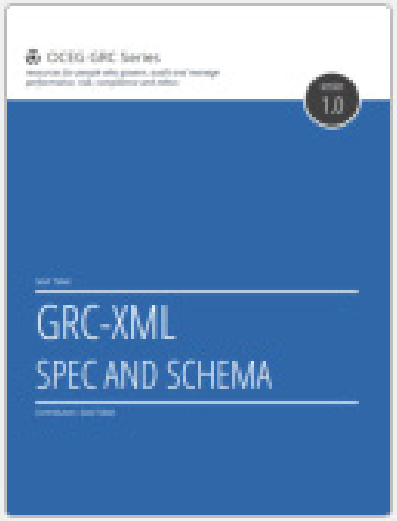


GRC Assessment Tools (Burgundy Book)

The purpose of the Burgundy Book is to provide GRC professionals, as well as those responsible for providing assurance, with a common set of assessment procedures that align with the OCEG GRC Capability Model™ ("Red ...

GRC Technology Solutions Guide

The GRC Technology Solutions Guide identifies and defines categories of technology that have a role in supporting the GRC system and specifically the Elements of the GRC Capability Model™. The Guide categorizes these Technology Categories ...



GRC-XML Spec and Schema

GRC-XML Risk and Control Taxonomy Version 1.0GRC-XML is a family of languages for Governance, Risk, and Compliance information sharing, integration, and communication. It is based on XBRL and XBRL Global Ledger Framework (XBRL GL). GRC-XML has ...

OCEG's GRC Certification, Surveys & Illustrations

OCEG has a range of resources that help organizations understand, apply, and communicate Principled Performance and GRC.

Certifications

GRC CERTIFY PROFESSIONAL
GRCP CERTIFICATION

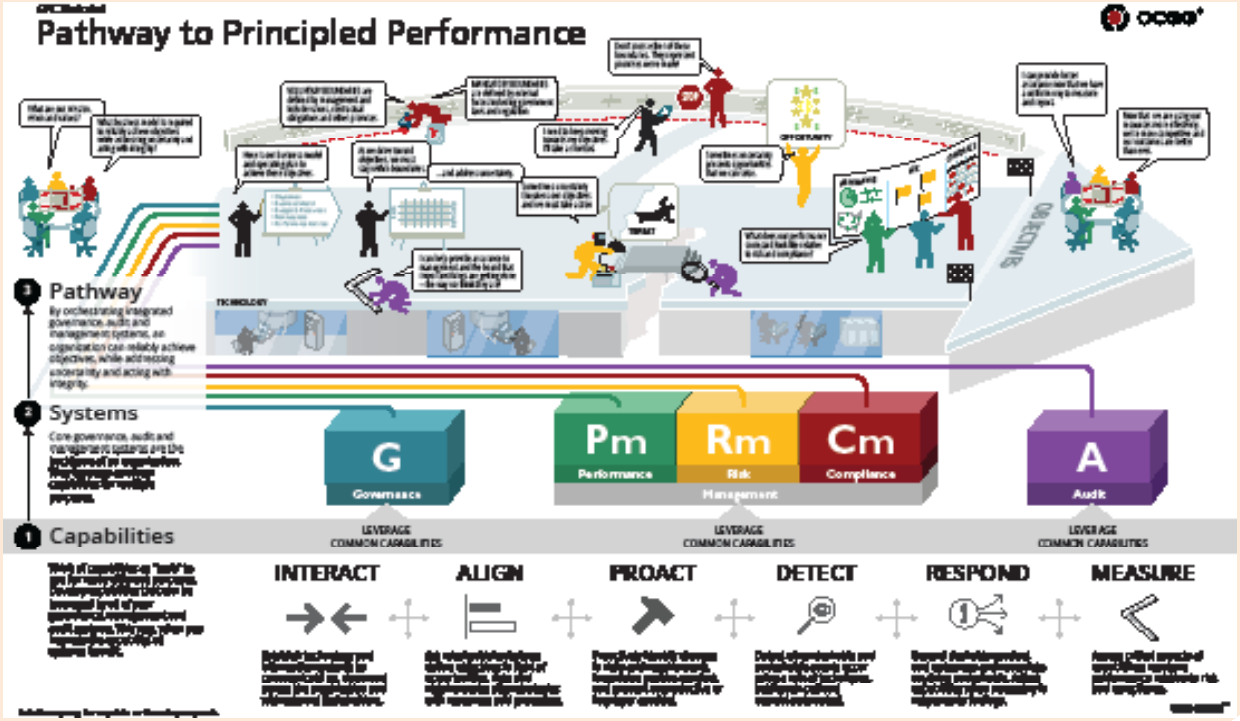
GRC CERTIFY AUDITOR
GRCA CERTIFICATION

Surveys

- OCEG One-Minute Polls on Focused Subjects
- GRC Maturity
- GRC Metrics & Measurement
- GRC Technology Strategy

GRC Illustrated

- OCEG has developed over 60 GRC illustrations that are info-graphics to help organizations understand and communicate Principled Performance and GRC.



OCEG's Supporters

Business executives from these great organizations and tens of thousands of others around the world are part of the OCEG community… join them today!

OCEG Star Supporters . . .

acl · BAKER HUGHES · convercent · DELL · Deloitte. · grc 20/20 · hiperos · Littler · MetricStream · Raytheon · RSA Archer GRC · SAP · THOMSON REUTERS ACCELUS · U.S. Cellular · Walmart

GRC Solution Council Members . . .

BAKER TILLY · compli cool. calm and compliant. · ControlPanel GRC · Wolters Kluwer · mega · NAVEX GLOBAL The Ethics and Compliance Experts · protiviti · STEELE · THE Network · TRUSTe · Workiva

Contact us

www.OCEG.org

4835 E. Cactus Road, Suite 225
Scottsdale, Arizona 85254
United States of America

info@OCEG.org
@OCEG
+1 (602) 234-9278